What is the Startup folder?

The Startup folder is a Windows directory whose contents (usually shortcuts) are launched automatically when a user logs in. Each user has one, and there is an all-users one. Attackers drop a shortcut or executable pointing at their payload, and it runs at every logon, requiring no admin for the per-user folder. It is one of the oldest and simplest persistence methods, easy to set and easy to inspect. It maps to MITRE T1547.001.

HOW IT WORKS

01 The technique and payload

The attacker drops a launcher into the Startup folder:

- Copy a payload or a `.lnk` shortcut into `shell:startup` (per-user, no admin) or the common Startup folder (all users, admin).
- The shortcut can point at the payload, a script, or a LOLBIN that fetches and runs it.
- It executes at the next (and every) logon for that user.

It is trivial to set up and needs no special privilege for the per-user folder. Documented for defensive context.

> NO ADMIN, VERY VISIBLE
>
> *The Startup folder needs no admin for per-user persistence, but it is also highly visible, just files in a known directory. Attackers use it for quick footholds and pair it with stealthier methods.*

HOW TO DEFEND

- Monitor the Startup folders (per-user and common) for new files and shortcuts.
- Baseline legitimate startup items so additions stand out (autoruns enumerates them).
- Use application allow-listing so a dropped payload cannot execute.
- Inspect shortcut targets, attackers hide LOLBINs and scripts behind innocent-looking `.lnk` files.
- Limit local admin to block the all-users Startup folder.

SOURCES

[1] MITRE ATT&CK: Boot or Logon Autostart Execution (T1547)

[2] Microsoft: Windows known folders

[3] MITRE ATT&CK: Persistence (TA0003)

Find the backdoors an attacker would leave behind.

securelayer7.net/learn/persistence/what-is-the-startup-folder

Open online